PENGAMANAN VIRTUAL NETWORK BERBASIS OPENVPN DENGAN KERBEROS PADA UBUNTU 14.04 LTS

Disusun sebagai salah satu syarat menyelesaikan Program Studi Strata I pada Jurusan Informatika Fakultas Komunikasi dan Informatika

Oleh:

ANGGA SATRIA BIMA

L 200 120 112

PROGRAM STUDI INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2016

HALAMAN PERSETUJUAN

PENGAMANAN VIRTUAL NETWORK BERBASIS OPENVPN DENGAN KERBEROS PADA UBUNTU 14.04 LTS

PUBLIKASI ILMIAH

oleh:

ANGGA SATRIA BIMA

L 200 120 112

Telah diperiksa dan disetujui untuk diuji oleh:

Dosen Pembimbing

Helman Muhammad, S.T., M.T.

NIK.1564

HALAMAN PENGESAHAN

PENGAMANAN VIRTUAL NETWORK BERBASIS OPENVPN DENGAN KERBEROS PADA UBUNTU 14.04 LTS

OLEH

ANGGA SATRIA BIMA

L 200 120 112

Telah dipertahankan di depan Dewan Penguji
Fakultas Komunikasi Dan Informatika
Universitas Muhammadiyah Surakarta
Pada hari Sabtu, 15 Oktober **2016**
dan dinyatakan telah memenuhi syarat

Dewan Penguji:

1. **Helman Muhammad, S.T.,M.T.** (.....)
   (Ketua Dewan Penguji)
2. **Dr. Ir. Bana Handaga, M.T.** (.....)
   (Anggota I Dewan Penguji)
3. **Dr. Heru Supriyono, M.Sc.** (.....)
   (Anggota II Dewan Penguji)

Publikasi ilmiah ini telah diterima sebagai salah satu persyaratan
Untuk memperoleh gelar sarjana
Tanggal 07 - 11 - 2016
Mengetahui,

Dekan
Fakultas Komunikasi dan Informatika

Husni Thamrin, S.T., M.T., Ph.D.
NIK : 706

Ketua Program Studi
Informatika

Dr. Heru Supriyono, M.Sc.
NIK:970

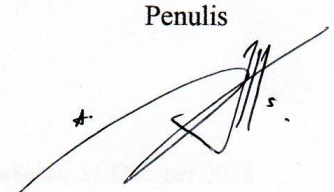
PERNYATAAN

Dengan ini saya menyatakan bahwa dalam naskah publikasi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali secara tertulis diacu dalam naskah dan disebutkan dalam daftar pustaka.

Apabila kelak terbukti ada ketidakbenaran dalam pernyataan saya di atas, maka akan saya pertanggungjawabkan sepenuhnya.

Surakarta, 15 Oktober 2016

Penulis



ANGGA SATRIA BIMA

L 200 120 112

UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA
Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: http://informatika.ums.ac.id. Email: informatika@ums.ac.id

SURAT KETERANGAN LULUS PLAGIASI

012/A.3-II.3/INF-FKI/I/2016

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Informatika menerangkan bahwa :

Nama	:	ANGGA SATRIA BIMA
NIM	:	L200120112
Judul	:	PENGAMANAN VIRTUAL NETWORK BERBASIS OPENVPN DENGAN KERBEROS PADA UBUNTU 14.04 LTS
Program Studi	:	Informatika
Status	:	**Lulus**

Adalah benar-benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi, dengan menggunakan aplikasi Turnitin.

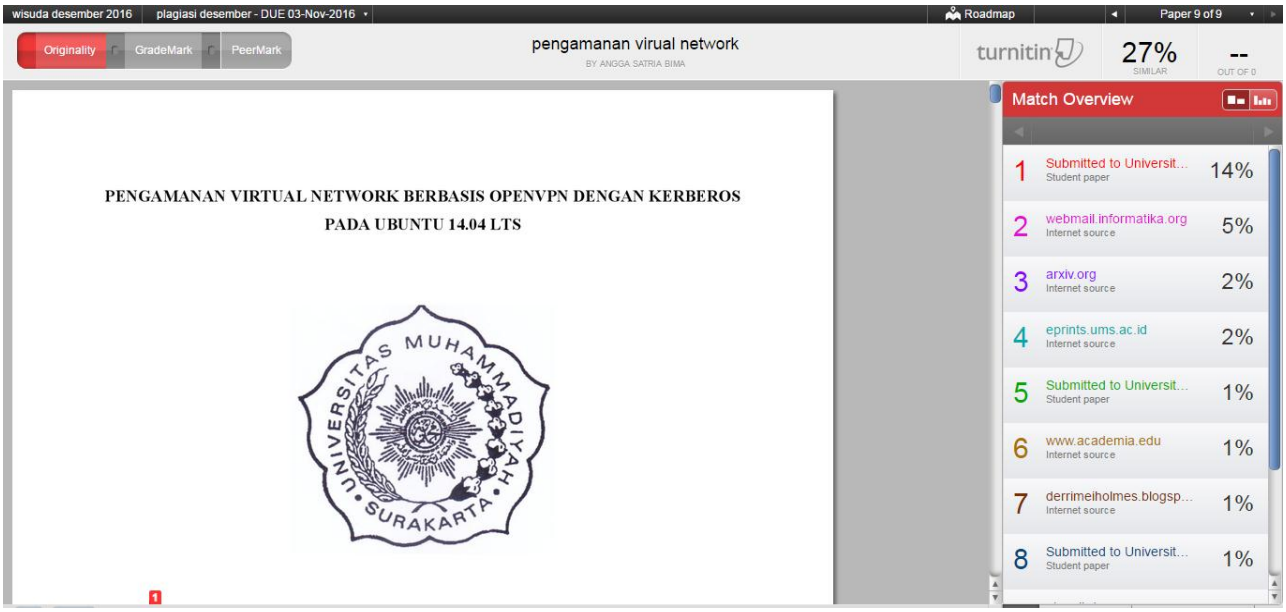
Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb

Surakarta, 31 Oktober 2016

Biro Skripsi Informatika

Ihsan Cahyo Utomo, S.Kom., M.Kom.


wisuda desember 2016
plagiasi desember - DUE 03-Nov-2016
Roadmap
Paper 9 of 9
Originality
GradeMark
PeerMark
pengamanan virual network
BY ANGGA SATRIA BIMA
turnitin
27%
SIMILAR
--
OUT OF 0
PENGAMANAN VIRTUAL NETWORK BERBASIS OPENVPN DENGAN KERBEROS
PADA UBUNTU 14.04 LTS
UNIVERSITAS MUHAMMADIYAH SURAKARTA
Match Overview
1 Submitted to Universit... Student paper 14%
2 webmail.informatika.org Internet source 5%
3 arxiv.org Internet source 2%
4 eprints.ums.ac.id Internet source 2%
5 Submitted to Universit... Student paper 1%
6 www.academia.edu Internet source 1%
7 derrimeiholmes.blogsp... Internet source 1%
8 Submitted to Universit... Student paper 1%

PENGAMANAN VIRTUAL NETWORK BERBASIS OPENVPN DENGAN KERBEROS PADA UBUNTU 14.04 LTS

Abstrak

Virtual Private Network adalah salah satu solusi untuk mengamankan data yang berada di jaringan lokal yang terhubung dengan jaringan publik. Kerberos dapat digunakan untuk meningkatkan pengamanan pada sisi protokolnya, sehingga tercipta keamanan ganda pada jalur data serta protokolnya. Dalam penelitian ini Ubuntu 14.04 LTS dipilih sebagai server virtual untuk menjalankan *Virtual Private Network* dan *Kerberos*, yang kemudian diuji terhadap serangan *sniffing* dan dimonitor dengan Wireshark. Hasilnya menunjukkan bahwa keamanan ganda itu telah terwujud.

Kata Kunci : Virtual Private Network, Kerberos, Wireshark

Abstract

Virtual Private Network is one of the solutions to secure data which reside in a local network that is connected to a public network. Kerberos may be utilized to increase the security on the protocol side, hence creating double security on the data path and protocol. In this research Ubuntu 14.04 LTS was chosen as virtual server for deploying Virtual Private Network and Kerberos, which was then tested against siniffing attacks and monitored with Wireshark. The result shows that the double security has been materialized.

Kata Kunci : Virtual Private Network, Kerberos, Wireshark

1. PENDAHULUAN

Dengan bertambahnya kebutuhan akan keamanan data yang terhubung baik pada jaringan lokal maupun public, memicu meningkatnya ancaman pada sisi keamanan data itu sendiri. *Sniffing* menjadi salah satu teknik serangan yang paling banyak digunakan untuk melihat, mengandakan, serta merubah isi file. Teknik serangan ini juga mampu melihat *username* serta *password* dari *user* yang sedang melakukan komunikasi melalui jaringan *local* maupun *public*. (Sujana 2014).

Caesar (2014) dalam asbtraksi skripsinya yang berjudul "Penerapan Virtual Private Network Menggunakan Mikrotik Router Pada RS Immanuel Bandung" mendefinisikan VPN merupakan singkatan dari Virtual Private Network yang artinya membuat jaringan private secara virtual di atas jaringan publik (umum) seperti internet.

Dua (2013) dalam artikelnya berjudul "Replay Attack Preverention In Kerberos Authenticatioin Protocol Using Triple Password" mengatakan Kerberos adalah protokol otentikasi yang digunakan untuk mengotentikasi pengguna dalam lingkungan terdistribusi. Menggunakan protokol otentikasi Kerberos, klien dapat mengotentikasi dirinya ke beberapa server menggunakan password yang juga dikenal sebagai kunci rahasia jangka panjang. Klien menerima Ticket-Granting-Ticket (TGT) dari Authentication Service (AS) dan tiket ini dapat digunakan untuk beberapa layanan yang klien butuhkan.

Supriyono (2013) dalam penelitiannya yang berjudul "Penerapan Jaringan Virtual Private Network Untuk Keamanan Komunikasi Data Bagi PT. Mega Tirta Alami" memberikan kesimpulan dengan menggunakan metode PPTP pembangunan VPN di PT. Mega Tirta Alami dapat memberikan keamanan dengan adanya enkripsi di setiap komunikasi data dan memberikan username dan password sebagai pengenal untuk setiap branch.

Pranata (2015) dalam abstraksi skripsinya yang berjudul "Analisis Keamanan Protokol Secure Socket Layer" mengatakan Sniffing adalah teknik pemantauan setiap paket melintasi jaringan. Ancaman keamanan yang disajikan oleh sniffer adalah kemampuan mereka untuk menangkap semua paket yang masuk dan keluar melalui jaringan, yang meliputi password, username dan isu-isu sensitif lainnya. Packet sniffer menangkap data ditujukan ke perangkat lain, yang kemudian akan disimpan untuk analisis nantinya. Sniffing juga dapat digunakan oleh administrator sistem untuk memonitor jaringan dan memecahkan masalah dalam jaringan.

Wirdasari (2011) dalam abstraksi skripsinya yang berjudul "Mekanisme Sistem Otentikasi Pada Protokol Kerberos Versi 5" mengatakan sistem otentikasi Kerberos adalah salah satu solusi mengatasi serangan untuk keamanan jaringan yang telah menjadi kelemahan sistem otentikasi konvensional (password based). mekanisme otentikasi oleh Kerberos

dilakukan dengan menggunakan kunci pribadi yang dibagi (*shared*) antara klien dan server. Kunci pribadi dilepaskan oleh pihak ketiga yang terpercaya bersama-sama (dipercaya pihak ketiga). Username dan password dari klien yang tidak dikirim melalui jaringan adalah salah satu manfaat dari sistem otentikasi Kerberos. Penggunaan kunci sesi ini juga mampu meningkatkan keamanan komunikasi dengan protokol Kerberos.

Khairina (2011) dalam abstraksi skripsinya yang berjudul "Analisis Keamanan Sistem Login" mengatakan setelah dilakukan pengamanan pada sistem login kemudian dilakukan analisis keamanannya dengan menggunakan sebuah software yaitu Wireshark dan dapat dideteksi mana password yang dienkripsi dan yang tidak dienkripsi.

Penelitian ini membuat virtual server berbasis Ubuntu 14.04 LTS yang di konfigurasi sebagai server *Virtual Private Network* yang bertugas menyediakan pengamanan enkripsi SSL *(Secure Socket Layer)* dimana SSL disini diaplikasikan untuk ubuntu 14.04 x64 dengan enkripsi 2048 bit dan pada sisi server Kerberos menyediakan kunci rahasia berupa *Ticket-Granting-Ticket (TGT)* dari *Auhentication Service (AS),* dan dengan adanya Wireshark diharapkan mampu memonitoring seluruh paket data yang sedang berjalan dalam jaringan serta menguji serangan dengan metode *sniffing attack*. *Sniffing* adalah teknik pemantauan setiap paket melintasi jaringan. ancaman keamanan yang disajikan oleh *sniffer* adalah kemampuan mereka untuk menangkap semua paket yang masuk dan keluar melalui jaringan, yang meliputi *password, username* dan isu-isu sensitif lainnya. *Packet sniffer* menangkap data ditujukan ke perangkat lain, yang kemudian akan disimpan untuk analisis nantinya. Sniffing juga dapat digunakan oleh administrator sistem untuk memonitor jaringan dan memecahkan masalah dalam jaringan.

2. METODE

2.1 Alat dan Bahan

Peralatan utama dibagi menjadi dua bagian yakni perangkat keras (hardware) dan perangkat lunak (software). Hardware yang digunakan adalah laptop Acer E1-471 dengan sistem operasi Linux Ubuntu 14.04 LTS dan spesifikasi Proccesor Intel® Core™ i3, RAM 2GB dan HDD 500GB. Software yang digunakan untuk penelitian ini adalah Oracle VM VirtualBox, Linux Ubuntu 14.04 LTS, VPN OpenVPN, Kerberos, Wireshark, Chrome Browser/Mozilla Firefox.

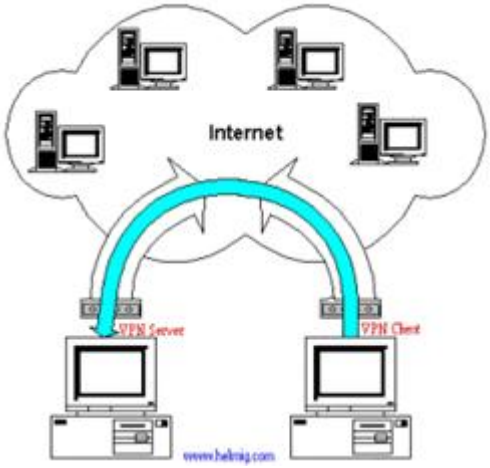
2.2 Perancangan dan Implementasi Server

a. Instalasi Virtual Private Network

1. Arsitektur VPN (OpenVPN)

Setelah semua aplikasi siap maka tahap berikutnya adalah mengkonfigurasi SSL (dalam kasus ini menggunakan openSSL). Langkah pertama adalah dengan membuat sub-direktori baru pada folder /etc/openvpn dengan nama folder ssl. Kemudian membuat certificate key yang baru dengan mengetikkan perintah "openssl hdparam –out /etc/openvpn/dh2058.pem 2048" pada root terminal.

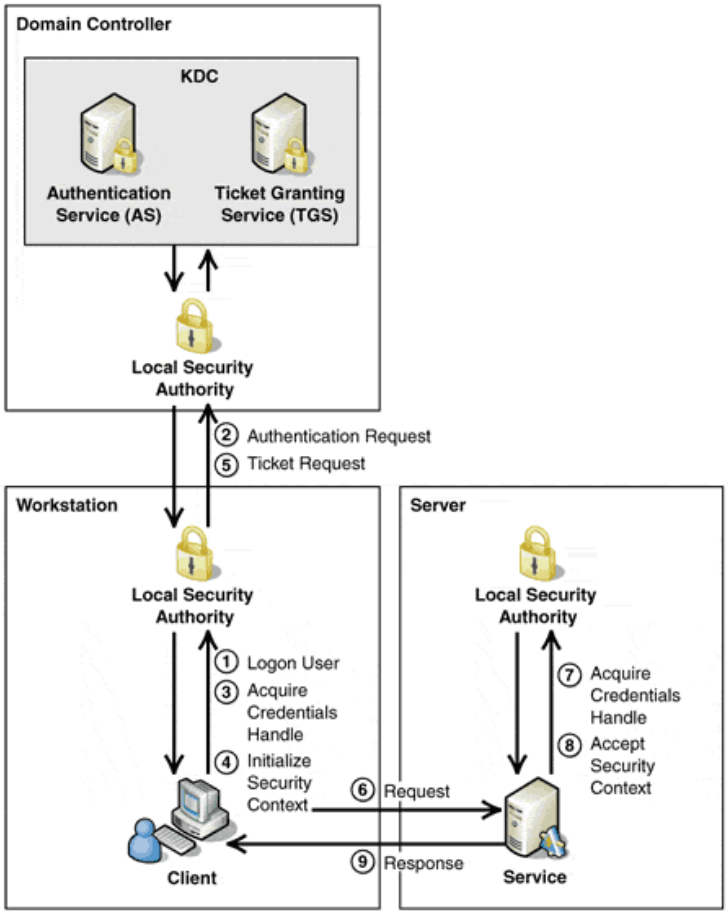
Setelah itu instal dan konfigurasi virtual private network dalam hal ini menggunakan OpenVPN sebagai salah satu pilhan yang disediakan oleh virtual private network.



Gambar 1. Ilustrasi arsitektur jaringan VPN dengan metode PPTP (diambil dari: http://teknodaninfokita.blogspot.com/2014/02/pengertian-vpn-dan-fungsinya.html)

b. Instalasi Kerberos

1. Arsitektur Kerberos



Gambar 1. Ilustrasi arsitektur Kerberos (diambil dari: http://madro99.blogspot.co.id/2009/11/mengamankan-sistem-dengan-kerberos.html)

2. Enkripsi

Data yang dikirim melalui jaringan dapat dirusak, dilihat, ataupun dimodifikasi isinya. Kerberos menyediakan otentikasi kriptografi melalui kombinasi penggunaan kunci rahasia dan enkripsi kuat. Kerberos menjamin integritas dan kerahasiaan data. Kunci rahasia adalah password yang diketahui oleh client atau server. Enkripsi dilakukan dengan algoritma kunci simetri dimana user diminta memasukkan password untuk melakukan login secara real time. Kunci simetri mengizinkan otentikasi dapat dilakukan secara real time karena karakteristiknya yang cepat. Algoritma kunci simetri menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi.

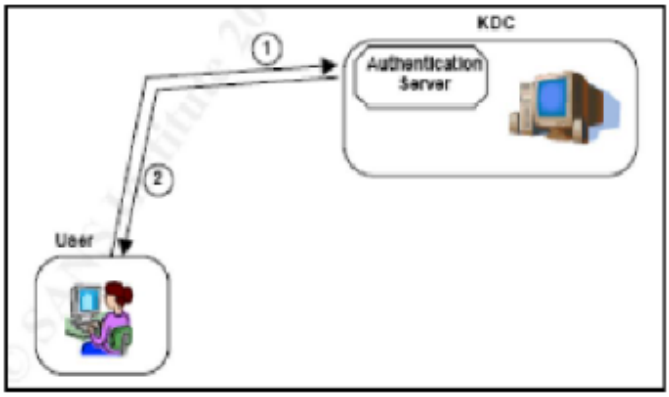
3. Key Distribution Center (KDC)

Protokol Kerberos digunakan untuk mengotentikasi principal dimana telah dijelaskan di atas bahwa principal adalah pihak yang identitasnya diverifikasi. Sebuah principal dapatlah merupakan user biasa, sebuah aplikasi server atau sebuah entitas

jaringan lainnya yang perlu diotentikasi. Pihak yang terlibat dalam proses otentikasi adalah:

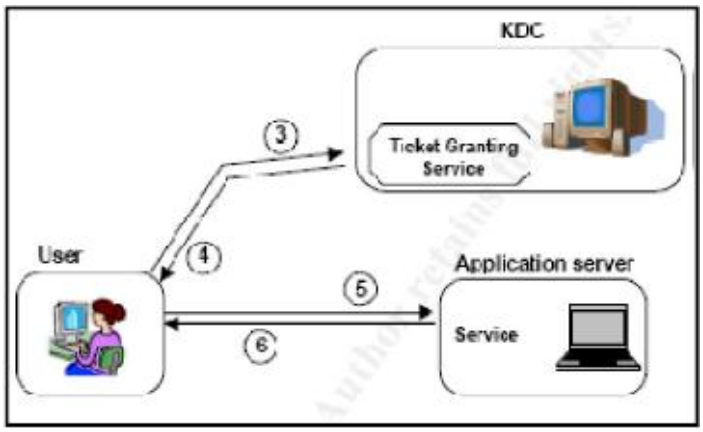
1. Client yang biasanya merupakan principal
2. Server yang biasanya merupakan verifier
3. Server Kerberos (KDC)

KDC adalah server Kerberos yang bertugas mendistribusikan session key kepada server dan client agar dapat melakukan koneksi, mengotentikasi server dan client, serta memudahkan client untuk melakukan koneksi kepada lebih dari satu server. Tugas untuk mengotentikasi principal dan memberikan session key kepada principal oleh KDC dilakukan melalui Authentication Service (AS), sedangkan tugas untuk memudahkan client melakukan koneksi dengan satu atau lebih server aplikasi dilakukan melalui Ticket Granting Service (TGS).



Gambar 2. Authentication Service

2. Ticket Granting Ticket (TGT) yang telah diterima pada saat authentication service. TGT ini digunakan untuk mengecek nama client dan session key (SA, KDC). Apabila session key-nya salah maka KDC tidak dapat mendekripsi authenticator. TGT juga digunakan untuk mengecek masa berlakunya otentikasi.



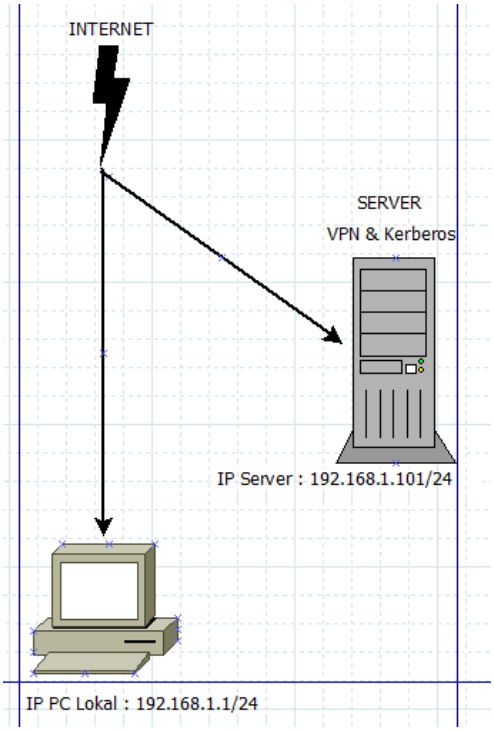
Gambar 3. Ticket Granting Service

4. Realms

Kerberos mempunyai kemampuan untuk membagi jaringan didalam grup-grup yang disebut “realms”. Paling sedikit terdapat satu realm dalam KDC. Pembagian ini dilakukan untuk menghindari terlalu banyaknya permintaan terhadap satu KDC.. Sebuah principal yang terdapat pada suatu realm dapat menghubungi sebuah server yang berada pada realm yang lain dengan menggunakan kemampuan otentikasi antar realm, yaitu:

1. Pertama-tama client meminta TGT dari KDC lokal untuk membuka koneksi dengan remote KDC dimana server yang dituju berada.
2. Setelah memperoleh TGT tersebut, client mengirimkan TGT tersebut kepada remote KDC dan meminta untuk dapat melakukan koneksi kepada server yang dituju
3. Setelah diotentikasi oleh remote KDC maka client mengirimkan authenticator dan server ticket kepada server yang dituju. Cara ini memungkinkan Kerberos menangani otentikasi ke semua server di jaringan, walaupun dalam realm yang berbeda-beda.

Dalam perancangan jaringan ini akan dibuat topologi jaringan sebagai berikut dimana client dapat mengakses server dari jarak jauh dengan terhubung melalui internet :



Gambar 4. Topologi Jaringan VPN dan Kerberos

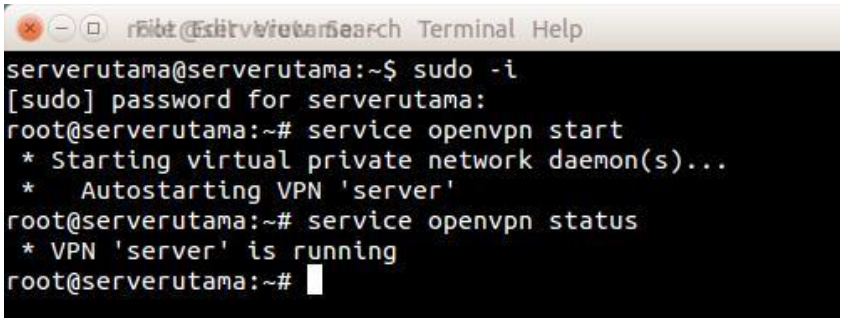
3. HASIL DAN PEMBAHASAN

3.1 Hasil Penelitian

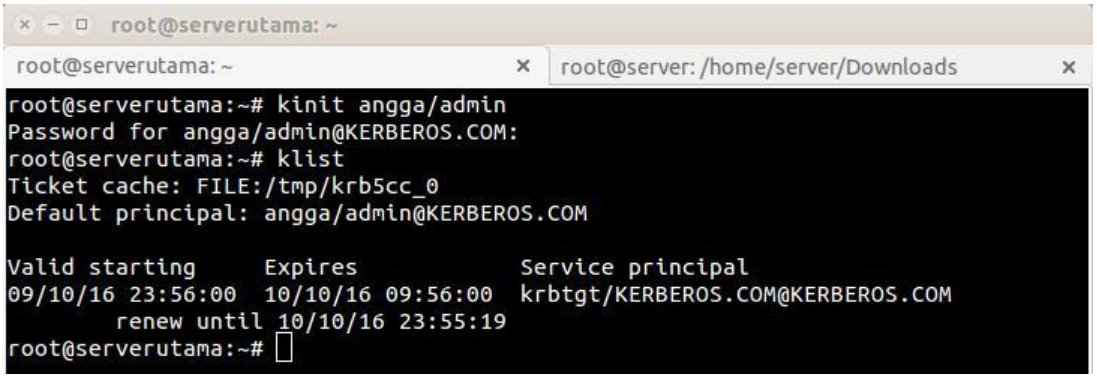
Setelah melakukan perancangan sistem mulai dari tahap pembuatan server VPN menggunakan OpenVPN sampai membuat server Kerberos dan juga melakukan monitoring Wireshark, selanjutnya menguji server VPN dan Kerberos dengan dilakukan 2 tahapan yaitu tahap mengaktifkan server VPN dan server Kerberos, selanjutnya tahap penyerangan (*sniffing*) dan monitoring menggunakan Wireshark.

a. Tahapan Mengaktifkan Server VPN dan Server Kerberos

Pada tahap ini server VPN dan server Kerberos diaktifkan, diawali dengan mengaktifkan server VPN terlebih dahulu selanjutnya mengaktifkan server Kerberos. File yang bernama client.ovpn yang berada pada sisi client diaktifkan dengan perintah **openvpn client.ovpn** maka ketika berhasil akan mendapat respon **Initialization Sequence Complete.** Setelah itu aktifkan server Kerberos dengan perintah **kinit angga/admin** lalu masukan password lalu lihat apakah server telah berjalan dengan perintah **klist**. Maka akan tampil valid starting yang menandakan tanggal dan pukul berapa server diaktifkan atau dimulai, lalu expires yang menandakan bahwa sampai kapan berlaku TGT dari AS Kerberos tersebut, serta service principal merupakan sebuah aturan yang telah dibuat sedemikian rupa bahwa hanya user atau pengguna yang diberikan hak akses berupa ticket yang mampu masuk pada server Kerberos tersebut.



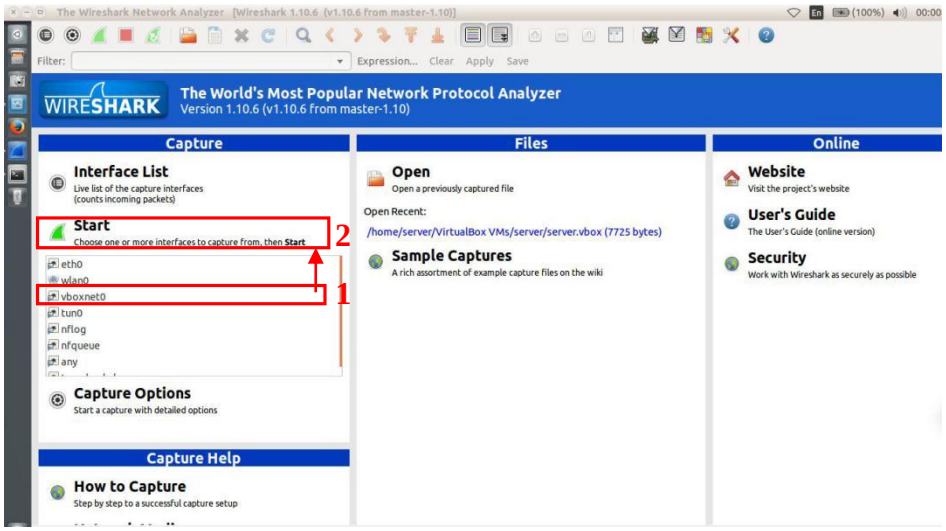
Gambar 5. Server VPN Running



Gambar 6. Server Kerberos Running

b. Tahapan Serangan (*sniffing*) dan Monitoring Wireshark

Penyerangan menggunakan teknik *sniffing* pasif ditujukan untuk melihat ip address dari server dan client ketika saling berkomunikasi melalu jaringan lokal maupun ketika terhubung dengan jaringan publik. Dengan memilih dan menjalankan device yang akan di *capture*, maka secara otomatis Wireshark akan melakukan *capture packet* data dan protokol yang sedang berjalan pada jaringan tersebut.

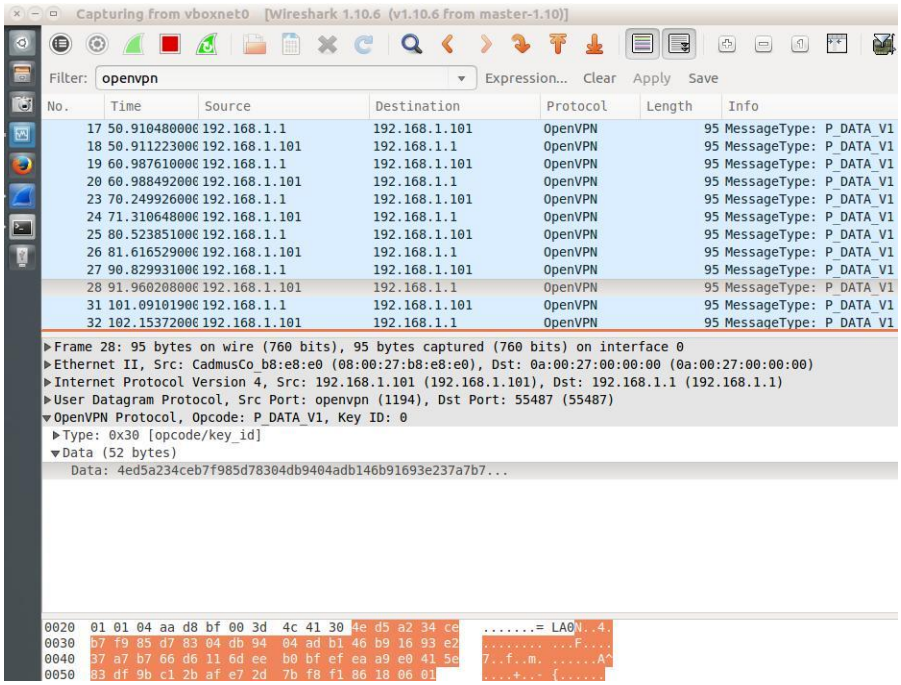


Gambar 7. *Interface Wireshark*

Filtering protokol yang akan dituju untuk memudahkan dalam melihat ip address, packet data serta protokol yang sedang berjalan pada jaringan lokal atau publik yang terenkripsi oleh OpenVPN.

Gambar 8. Melakukan Filter Protokol OpenVPN

Maka akan ditampilkan secara visual capturing dari ip 192.168.1.1 (klien) menuju 192.168.1.101 (server) ataupun sebaliknya secara terus menerus.



Gambar 9. Hasil Capturing Packets Data Terenkripsi

3.2 Pembahasan

Virtual Private Network pada dasarnya layanan yang diberikan untuk mengamankan jaringan lokal yang terhubung melalui jaringan publik. SSL menawarkan komunikasi yang aman ditentukan oleh pemilihan suite cipher. Suite cipher itu sendiri telah mendapat empat komponen dan teknik untuk pertukaran kunci, otentikasi, enkripsi dan metode untuk menghitung pesan mencerna hash. OpenSSL yang digunakan yaitu dengan 2048 bit.

Kerberos merupakan layanan keamanan yang dikembangkan untuk mengamankan protokol dengan mensetting Ticket-Grenting-Ticket dari Authentication Service, dengan begitu akses menuju server dapat diproteksi dengan maksimal.

Wireshark merupakan tools network analyzer dan capturing packet secara visual dengan fasilitas yang cukup lengkap untuk melihat jalur data serta protokol yang digunakan, dengan aplikasi Wireshark dapat digunakan untuk melakukan serangan dengan metode snffing baik dengan sniffing aktif maupun pasif, dan memonitor dengan tujuan memperbaiki sebuah sistem jaringan yang sedang berjalan.

4. PENUTUP

A. Kesimpulan

Dari serangkaian penelitian yang telah dilakukan, dapat diambil kesimpulan yang mendasarkan pada kegiatan sebagai berikut :

1. Kerberos dapat memberikan pengamanan tambahan kepada jaringan VPN. Hal ini disebabkan karena user harus memiliki *Ticket-Granting-Ticket* (TGT) yang diberikan oleh *Authentication Service* (AS) untuk mengakses server, sehingga ketika user tidak memiliki *Ticket-Granting-Ticket* (TGT) maka user tidak dapat masuk pada server tersebut.
2. Dalam penelitian ini server Kerberos belum sampai tahap dapat dimonitor oleh aplikasi Wireshark, sehingga untuk melakukan monitoring Kerberos pada Wireshark hanya digunakan terminal sebagai tanda bahwa Ticket-Granting-Ticket (TGT) dari Authentication Service (AS) telah aktif.

B. Saran

Saran dari penulis untuk pengembang berikutnya adalah, agar dilakukan perbaikan script sehingga user baru dapat langsung melakukan monitoring melalui aplikasi Wireshark secara visual.

DAFTAR PUSTAKA

Caesar, Y. (2014, August 23). Penerapan Virtual Private Network menggunakan Mikrotik Router Pada RS Immanuel Bandung. Tugas Akhir, Sekolah Tinggi Manajemen Informatika dan Ilmu Komputer lpkia Bandung.

Dua, G., Gautam, N., Sharma, D., & Arora, A. (2013). Replay Attack Prevention in Kerberos Authentication Protocol using Triple Password. *International Journal of Computer Networks & Communications*, 5(2), 59-70. doi:10.5121/ijcnc.2013.5205

Sujana, A. P. (2014). Perangkat Pendukung Forensik Lalu Lintas Jaringan. Jurnal Teknik Komputer Unikom, *3*(1).

Pranata, H., Abdillah, L. A., & U. E. (2015). Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan. Proceeding.Student Colloquium Sistem Informasi & Teknik Informatika (SC-SITI). Skripsi, Fakultas Ilmu Komputer. Universitas Bina Darma Palembang.

Supriyono, H., Widjaya, J. A., & A. S. (2013, September). Penerapan Jaringan Virtual Private Network Untuk Keamanan Komunikasi Data Bagi PT. Mega Tirta Alami. WARTA, 16(2), 88-101.

Wirdasari, D. (2011). Mekanisme Sistem Otentikasi Pada Protokol Kerberos Versi 5. Jurnal Program Studi Ilmu Komputer, Universitas Sumatera Utara.

.

Khairina, D. M. (2011, July). Analisis Keamanan Sistem Login. Skripsi, Program Studi Ilmu Komputer, FMIPA Universitas Mulawarman Samarinda.